



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/004,081	10/30/2001	David M. Blaker	9269-9	9375
20792	7590	07/01/2005	EXAMINER	
MYERS BIGEL SIBLEY & SAJOVEC			PICH, PONNOREAY	
PO BOX 37428			ART UNIT	
RALEIGH, NC 27627			PAPER NUMBER	
2135				
DATE MAILED: 07/01/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/004,081	BLAKER, DAVID M.
	Examiner	Art Unit
	Ponnoreay Pich	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 30 October 2001.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-33 is/are pending in the application.
4a) Of the above claim(s) 10-15 is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-9 and 16-33 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) 10-15 are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 30 October 2001 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 3/02, 6/02, and 10/04
4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
5) Notice of Informal Patent Application (PTO-152)
6) Other: ____.

DETAILED ACTION

Claims 1-33 have been examined and are pending.

Election/Restrictions

Restriction to one of the following inventions is required under 35 U.S.C. 121:

- I. Claims 1-9 and 16-33, drawn to generating a random number for a stream cipher, classified in class 380, subclass 42.
- II. Claims 10-15, drawn to determining random values via the use of a state machine circuit, classified in class 380, subclass 251.

Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention II has separate utility such as a generic random number generator for an electronic gaming system. See MPEP § 806.05(d).

Because these inventions are distinct for the reasons given above and the search required for Group II is not required for Group I, restriction for examination purposes as indicated is proper.

During a telephone conversation with Mr. Scott Moore (919-854-1400), who works at the same law firm as Mr. Timothy O'Sullivan and is taking over the case from Mr. O'Sullivan, on 6/20/2005 an election was made without traversal to prosecute the invention of the elected Group I, claims 1-9 and 16-33. Affirmation of this election must be made by applicant in replying to this Office action. Claims 10-15 are withdrawn from

further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Information Disclosure Statement

In the IDS filed 1/14/2003, the examiner did not consider the Bruce Schneier document submitted as it fails to list a publication date, see 35 CFR 1.98. The rest of the IDS submitted by the applicant were considered.

Specification

The use of the trademark ARC-4 and RC-4 on page 1 have been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Objections

Claims 1, 16, and 25 are objected to because of the following informalities: The claims should recite "...a stream cipher..." instead of "...an stream cipher...." Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 3-5, 7-9, 18-20, 22-24, 27-29, and 31-33 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claims 3, 7, 18, 22, 27, and 31 recite "... comparing values of counters utilized determining the at least two sequential random values...." This limitation seems to be incorrectly worded, thus rendering the claims indefinite. It is unclear if the determining is a result of the comparing or if the counters are utilized in determining.
2. Any claims not specifically addressed are rejected by virtue of dependencies.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-9 and 25-33 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 1:

Claim 1 refers to a software method of determining random values for a stream cipher, comprising a determining step which can be implemented in software alone and utilizing a software common S-box. Note that on page 6, lines 20-23 of the

specification, the applicant stated that the applicant's invention could be implemented entirely with software. Software by itself is not statutory and must be accompanied by some form of hardware to be statutory.

Claims 2-9:

Claims 2-9 are dependent on claim 1 and merely further defines the software determining step of claim 1. As such, claims 2-9 are also directed towards non-statutory subject matters.

Claim 25:

Claim 25 refers to a computer program product comprising a computer readable media having computer readable program code embodied therein and computer readable program code. The examiner notes that on page 6, lines 31-33, the applicant defines a computer-readable medium as including "an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or propagation medium." As such, the computer-readable media recited in claim 25 reads on a propagation signal, which is not tangible, and thus is non-statutory. Further, a computer readable program code is just software which is not statutory. Thus, the computer program product recited in claim 25 is not directed towards any statutory subject matter.

Claims 26 and 27:

Claims 26 and 27 merely further define the computer readable program code recited in claim 25 and still do not recite any statutory subject matter.

Claim 28:

Claim 28 further defines the computer readable program code recited in claim 25.

In addition, claim 28 also recites at least two software states and a software counter.

Nothing statutory was recited.

Claims 29-31:

Claims 29-31 merely further define the computer readable program code recited in claim 25 and still do not recite any statutory subject matter.

Claim 32:

Claim 32 further defines the computer readable program code recited in claim 25.

In addition, claim 32 also recites at least two software states and a software counter.

Nothing statutory was recited.

Claims 33:

Claim 33 merely further defines the computer readable program code recited in claim 25 and still does not recite any statutory subject matter.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 16, and 25 are rejected under 35 U.S.C. 102(e) as being anticipated by Venkatesan et al (US 6,490,354).

Claim 1:

Venkatesan discloses a method of determining random values for a stream cipher comprising:

1. Determining at least two sequential random values in parallel utilizing a common S-box (Fig 6; col 9, lines 31-57; and col 11, lines 22-25).

Note that the only way for Venkatesan's invention to operate on a word level is by operating in parallel. Also note that an S-box is anything which gives an output that is different than the input. Therefore, the S-box recited in claim 1 can reads on just the S array disclosed by Venkatesan, just the G array, or the combination of the S and G arrays.

Claims 16 and 25:

Claims 16 and 25 recite limitations substantially similar to claim 1. The difference is that claim 16 refers to a system and claim 25 refers to a computer program product with means and computer readable media having computer readable program code therein, the computer readable program code comprising computer readable program code configured to implement the method of claim 1.

Another difference is that claims 16 and 25 explicitly recite a memory containing an S-box. This limitation is inherent to Venkatesan's invention as Venkatesan discloses

that the array(s) used for the S-box are initialized and the contents updated (col 10, line 8-col 11, line 5).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 2-3, 6-7, 17-18, 21-22, 26-27, and 30-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatesan et al (US 6,490,354) in view of Klug et al (US 5,528,526).

Claims 2, 17, and 26:

Claims 17 and 26 are substantially similar to claim 2. Claim 17 differs from claim 2 in that claim 17 recites a system with means for implementing the method of claim 2. Claim 26 differ in that it recites a computer program product with computer readable program code for implementing the method of claim 2.

As per claims 2, 17, and 26, Venkatesan further discloses accesses of the common S-box utilized to determine a first of the two sequential random values and access of the common S-box utilized to determine a second of the two sequential random values (Fig 6; col 9, lines 31-57; and col 11, lines 22-25). Venkatesan's

invention is used with a stream cipher, so the numbers in the stream of numbers generated by Venkatesan's random number generator are all random numbers.

Venkatesan does not disclose:

1. Determining if a collision exists between accesses.
2. Modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the common S-box.

However, Klug discloses determining if a collision/cycle exists between in the generation of random numbers (col 3, lines 21-35). Note that each symbol disclosed by Klug in the pattern supplied on bus 18 reads on a random number. In light of this, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Venkatesan's invention to determine if a collision exists between accesses of the common S-box utilized to determine a first of the two sequential random values and access of the common S-box utilized to determine a second of the two sequential random values. One of ordinary skill would have been motivated to do so as Klug discloses that by detecting short cycle patterns (collisions), many diverse failure modes associated with random number generators may be identified.

Klug also does not explicitly disclose modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the common S-box. However, this limitation is obvious to the combination of Venkatesan and Klug as the reason Klug wanted to detect collision or repeating

patterns in random number generation was to determine if an error is present in the generation process. If an error is present, it is obvious to one of ordinary skill to modify the determination of the random values as recited in claims 2, 17, and 26. One of ordinary skill would have been motivated to modify the determination, as it would correct the errors disclosed by Klug.

Claims 6, 21, and 30:

Claims 21 and 30 are substantially similar to claim 6. Claim 21 differs from claim 6 in that claim 21 recites a system with means for implementing the method of claim 6. Claim 30 differ in that it recites a computer program product with computer readable program code for implementing the method of claim 6.

As per claims 6, 21, and 30, Venkatesan does not disclose:

1. Determining if a collision exists between accesses of the common S-box utilized to determine a first portion of the first of the two sequential random values and accesses of the common S-box utilized to determine a second portion of the first of the two sequential random values.
2. Determining if a collision exists between accesses of the common S-box utilized to determine a first portion of the second of the two sequential random values and accesses of the common S-box utilized to determine a second portion of the two sequential random values.

However, the above limitations are obvious to the combination of Venkatesan and Klug. Venkatesan's invention deals with generating a stream of random numbers

(in byte format) for encryption purposes (col 1, lines 9-12). Klug deals with detecting collisions or pattern repeats within a sequence of numbers/symbols (col 1, lines 8-12). It is obvious that the combination invention of Venkatesan and Klug would be able to detect collisions within any random value comprising a first and second portion as the combination invention looks for collisions within the streams itself rather than just one number with another number. The examiner also notes that within the stream generated, it is arbitrary where one “number” begins and ends as it depends on the system the random number generator is used how many bits or bytes comprise a number.

Claims 3, 7, 18, 22, 27, and 31:

Venkatesan does not disclose:

1. Determining a state associated with the determination of the at least two sequential random values.
2. Comparing values of counters utilized determining the at least two sequential random values.
3. Detecting a collision based on the determined state and the compared values.

However, the above limitation is obvious to the combination invention of Venkatesan and Klug. Klug discloses that once a collision is first detected, more tests are needed to determine if the collision is a false repeat or not (Fig 2; Fig 5; and col 6, line 45-col 7, line 40). Each level of testing for a match reads on a separate state as disclosed by Klug. To determine absolutely that the pattern detected is not a false

collision, the state must be determined to be the final level of verification (Fig 5, items 82 and 84).

Allowable Subject Matter

Claims 4-5, 8-9, 19-20, 23-24, 28-29, and 32-33 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

Claims 4, 19, and 28:

The examiner did not find teachings in the prior art *wherein the step of detecting a collision comprises the steps of:*

1. *Detecting a first collision if the determined state is the first state and the second i counter values equals the first j counter value.*
2. *Detecting a collision if the determined state is the first state and the second j counter value equals the first i counter value.*
3. *Detecting a third collision if the determined state is the first state and the second j counter values equals the first j counter value.*
4. *Detecting a fourth collision if the determined stat is the second state, the second j counter values equals the first t counter value.*

5. *Detecting a fifth collision if the determined state is the second state and the second t counter values equals the first i counter value and the second j counter value is not equal to the first i counter value.*

Claims 8, 23, and 32:

The examiner did not find teachings in the prior art wherein *determining if a collision exists...comprises the steps of:*

1. *Detecting a first collision if the determined state is the second state and the first i counter value equals the first t counter value.*
2. *Detecting a second collision if the determined state is the second state and the second t counter value equals the second i counter value.*

Claims 5, 9, 20, 24, 29, and 33:

Claims 5, 9, 20, 24, 29, and 33 depends on claims that were indicated as allowable above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PP


Primary Examiner
Art Unit 2135